



Runtime randomization and perturbation for virtual machines.

JAVIER CABRERA ARTEAGA

Licentiate Thesis in [Research Subject - as it is in your ISP]
School of Information and Communication Technology
KTH Royal Institute of Technology
Stockholm, Sweden [2022]

TRITA-ICT XXXX:XX
ISBN XXX-XX-XXXX-XXX-X

KTH School of Information and
Communication Technology
SE-164 40 Kista
SWEDEN

Akademisk avhandling som med tillstånd av Kungl Tekniska högskolan framlägges till offentlig granskning för avläggande av licentiatexamen i [ämne/subject] [veckodag/weekday] den [dag/day] [månad/month] [år/2022] klockan [tid/time] i [sal/hall], Electrum, Kungl Tekniska högskolan, Kistagången 16, Kista.

© Javier Cabrera Arteaga, [month] [2022]

Tryck: Universitetsservice US AB

Abstract

Write your abstract here...

Keywords: Keyword1, keyword2, ...

Sammanfattning

Write your Swedish summary (popular description) here...

Keywords: Keyword1, keyword2, ...

Acknowledgements

Write your professional acknowledgements here...

Acknowledgements are used to thank all persons who have helped in carrying out the research and to the research organizations/institutions and/or companies for funding the research.

Name Surname,
Place, Date

[Personalizado iconos creados por monkik - Flaticon](https://www.flaticon.es/iconos-gratis/personalizado "personalizado iconos")

[Computadora iconos creados por Freepik - Flaticon](https://www.flaticon.es/iconos-gratis/computadora "computadora iconos")

Contents

Contents	vi
1 Introduction	1
1.1 Research questions	2
1.2 Contributions	2
1.3 Publications	3
2 Background & State of the art	7
2.1 WebAssembly overview	7
2.1.1 From source to Wasm	8
2.1.2 WebAssembly specification	9
2.1.3 WebAssembly security	12
2.2 Software Diversification	12
2.2.1 Variants' generation	13
2.2.2 Variants' equivalence	14
2.2.3 Usages of Software Diversity	15
2.3 Open challenges	17
3 Technical contributions	21
3.1 Artificial Software Diversity for WebAssembly	21
3.2 CROW: Code Randomization Of WebAssembly	23
3.3 MEWE: Multi-variant Execution for WEbAssembly	26
4 Methodology	31
4.1 Corpora	31
4.2 RQ_1 . To what extent can we artifically generate program variants for WebAssembly?	33
4.3 RQ_2 . To what extent are the generated variants dynamically different?	36
4.4 RQ_3 . To what extent do the artificial variants exhibit different execution times on Edge-Cloud platforms?	38
5 Results	41

5.1	RQ_1 . To what extent can we artificially generate program variants for WebAssembly?	41
5.1.1	Program's populations	41
5.1.2	Challenges for automatic diversification	42
5.1.3	Properties for large diversification	43
5.2	RQ_2 . To what extent are the generated variants dynamically different?	44
5.2.1	Stack operation traces.	44
5.2.2	Execution times.	45
5.3	RQ_3 . To what extent do the artificial variants exhibit different execution times on Edge-Cloud platforms?	47
5.3.1	Execution times	48
6	Conclusion and Future Work	51
6.1	Summary of the results	51
6.2	Future work	51
6.2.1	wasm-mutate future work	51
	Bibliography	53

